Visa Security Alert

AUGUST 2020

PANDEMIC UNEMPLOYMENT ASSISTANCE FRAUD REMAINS PROLIFIC

Distribution: Public

1. Pandemic Unemployment Assistance Fraud

Pandemic unemployment assistance (PUA) fraud is a significant consequence of the ongoing COVID-19 pandemic and remains prolific as the pandemic persists. Visa Payment Fraud Disruption (PFD) previously identified the use of mobile payment applications to facilitate PUA fraud. Fraudsters use these mobile applications to either conduct fraudulent purchases with the ill-gotten unemployment benefits or contact prospective stimulus or unemployment benefit recipients with phishing emails that promise early delivery of the government-issued payment via the mobile payment applications. In the phishing campaigns, the actors request that the targeted individual provide sensitive personally identifiable information (PII) to receive an early benefit payment and then harvest the PII to conduct fraudulent activity. Additionally, PFD identified an increase in the recruitment of money mules through fraudulent work-from-home offers as a consequence of the high unemployment rate.

Throughout July 2020, PUA fraud continued, and PFD identified new tactics used by threat actors to conduct this fraud. In the most recent schemes, threat actors use a prepaid payment account service and a corresponding mobile application to monetize the stolen PUA funds. The scheme is similar to previous mobile application related fraud in that the threat actors obtain complete PII records, known colloquially in the underground as 'fullz', which generally contain the victim's full name, address, date of birth, social security number, driver license, and payment account information. Fullz are obtained through various compromises and subsequently bought and sold on the cybercrime underground.

The fullz are then used to fraudulently apply for PUA on government websites. As part of this process, the applicant is asked for a direct deposit account to which the funds will be deposited. After the actors register for a payment account and PUA benefits, and the funds are made available by the issuer, PFD believes the criminals will immediately proceed to conduct illicit purchases to effectively cash out the funds.

PFD identified tutorials and a significant amount of discussion on the cybercrime underground regarding the unemployment scheme, specifically targeting PUA. This current scheme is focused on U.S. PUA programs; however, similar tactics could be used to conduct fraud in other countries on various types of government-sponsored relief programs. The tutorials and discussions include tactics such as claiming the applicant is self-employed, the most effective salary range to maximize PUA payments, and which US states are easiest to target and still paying PUA. PFD also observed a significant increase in fraudulent purchases attributed to this unemployment scheme in July, which corresponds to an increase in cybercrime underground activity over

the same period. The fraudulent purchases occurred both domestically and cross-border and included purchases of cryptocurrency, gift cards, electronics, and other forms of person to person transfers. A significant amount of these fraudulent purchases occurred as contactless, payment entry mode 07, but also included magstripe entry mode 90 transactions. PFD also believes criminals conducted fraudulent card not present (CNP)/eCommerce transactions.

2. Conclusion

Evidence of such discussions and detailed tutorials suggests that multiple, disparate criminal actors are attempting these fraud techniques globally. As such, these schemes are not necessarily attributed to a single threat actor/group. PFD assesses that while there may be restrictions on international mailing of physical payment cards, actors utilizing virtual accounts to register and carry out these schemes can effectively do so globally. PFD expects threat actors to continue these attempts until they identify that controls are in place to mitigate these general techniques, effectively driving the fraudsters to explore other options.

PFD implements comprehensive monitoring within the payments ecosystem to identify, mitigate and prevent PUA fraud, and continues to closely monitor the payments ecosystem for novel and emerging fraud schemes that exploit the ongoing COVID-19 pandemic and associated unemployment programs. PFD will continue to extensively investigate these schemes and report notable developments to the payments ecosystem.

3. Recommendations for Issuers, Acquirers, Processors, Payment Application Financial Technology Payment Firms (FinTechs)

Financial institutions should directly contact respective state unemployment insurance agencies to determine the most appropriate method for returning fraudulent unemployment funds to the agencies. Visa also recommends the following best practices to reduce unemployment fraud.

Issuers:

- ensure the payment account device (if a virtual card) is associated with the known cardholder.
- as a form of validation and risk monitoring, verify the name on the deposit matches the name on the account.
- limit the number of payment accounts that can be loaded to a single device.
- monitor for multiple deposits from multiple states going to the same account.

Issuers, acquirers and processors:

- point-of-sale transactions that occur outside of the account holder's location should be flagged and treated as suspicious.
- implement transaction amount and velocity restrictions, at both the PAN and issuing (ISO) BIN level.
- monitor for suspicious monetization techniques, such as individuals conducting multiple purchases at a single location until an account is emptied. Previously inactive and newly established accounts that suddenly begin to transact in high volumes and amounts should also be treated as indicative of fraud.
- consider tiered usage of new accounts, and tiered disbursement tranches based on history of valid use of account.
- thoroughly review all cardholder authentication data.
- monitor for excessive declines or transaction activity outside the geographic area where the funds were disbursed.

Issuers and payment application FinTechs:

- institute effective know-your-customer (KYC) measures to ensure that initial registration for accounts are sufficiently reviewed.
- limit the number of payment accounts that can be loaded to a single device.
- monitor for discrepancies in geolocation data, such as inconsistencies between device IP, initial location of user at the time of registration, and location of transaction.

For more information, or for assistance with fraud identification and additional mitigation strategy recommendations, please contact **paymentintelligence@visa.com**